U N I V E R S I D A D A R T E M I S A

D E P A R T A M E N T O C I E N C I A S N A T U R A L E S

C A R R E R A L I C E N C I A T U R A E N E D U C A C I Ó N

B I O L O G Í A

C u r s o o p t a t i v o

L A S T I C E N E L P R O C E S O D E E N S E Ñ A N Z A A P R E N D I Z A J E D E L A B I O L O G Í A

4To a ñ o C R E , d e 4 y 5 a ñ o s , I s e m e s t r e

T o t a l d e h o r a s c l a s e s : 2 4 ; - - - s e g ú n l a s f o r m a s o r g a n i z a t i v a s y l a s t i p o l o g í a s d e c l a s e s

A u t o r a : M S . c . J u l i o C e s a r V a l h u e r d i C a b e z a

C u r s o 2 0 1 8 - 2 0 1 9

Fundamentación de la asignatura

En la asignatura de las TIC en el proceso de enseñanza aprendizaje de la Biología se puede apreciar el uso generalizado de las potentes y versátiles tecnologías de la información y las comunicaciones (TIC), experimentado significativos cambios que alcanzan todos los ámbitos de la actividad humana. En particular, en la esfera de la educación sus efectos se manifiestan de manera muy especial, pues si bien el desarrollo de las computadoras había permitido avances en su aplicación en la educación, fue hasta que se reunieron los avances de las computadoras con los avances de las telecomunicaciones, cuando las aplicaciones a la educación se multiplicaron y expandieron de manera considerable.

Es objetivo esencial consiste en preparar a los futuros profesores de Biología en los contenidos necesarios para impartir los programas de las escuelas Secundarias Básicas y de los Institutos Preuniversitarios en la integración de las TIC al proceso de enseñanza aprendizaje a través de la modalidad a distancia, posibilitando así su desarrollo profesional de manera que alcancen niveles de actuación que garanticen la competitividad institucional tanto en el entorno nacional como en el internacional

En general, la realización de esta asignatura parte de la necesidad de contribuir al logro del objetivo del perfeccionamiento de la enseñanza a través del uso e inclusión de las TIC en la educación, en particular con el empleo de hiperentornos de aprendizaje virtuales que permiten un mayor intercambio de contenidos y criterios entre los estudiantes, además de propiciar una mayor independencia y desarrollar los valores de responsabilidad y profesionalidad ante el cumplimiento del curso, el mismo abarcará a todos los profesores universitarios de la universidad de artemisa y está dirigida al proceso de instrucción – educación o sea a las tres áreas del conocimiento.

El contenido de esta asignatura propicia el desarrollo de habilidades generales y específicas relacionadas con el perfil profesional del egresado, contribuye a la formación y el desarrollo de la concepción científica del mundo al profundizar en el estudio TIC y su vinculación con la carrera de Biología. De igual manera favorece el trabajo de los Entornos de Aprendizajes Virtuales, profundizar desde el punto de vista educativo e instructivo en una base teórica y práctica que le permitan orientar correctamente a sus alumnos en las escuelas en cómo proporcionar las herramientas para el uso de estas tecnologías. La TIC se trabaja en la asignatura de forma integral y teniendo en cuenta su utilización son útiles en procesos industriales y en otras ramas de la economía.

Objetivos generales de la asignatura

Valorar las posibilidades que brinda la utilización TIC al proceso de enseñanza aprendizaje a través de la modalidad a distancia de estudiantes de la Universidad de Artemisa".

-

Plan temático

Tema 1.- Introducción a los fundamentos de la Seguridad Informática.

Tema 2.- La seguridad informática en las actividades cotidianas.

Tema 3.- Algunas configuraciones en herramientas y aplicaciones informáticas.

Tema 4.- Metodología para la implementación del programa de seguridad informática en las instituciones del MINED.

Dosificación del curso

Tema	Contenido
1	1. Conceptos de información y datos.
	2. Clasificación de la información según su importancia.
	3. Concepto de sistema informático.
	4. Concepto de seguridad Informática y sus principales objetivos.
	5. Conceptos de disponibilidad, confidencialidad e integridad de la información que se procesa, intercambie, reproduzca o conserve a través de las tecnologías informáticas, como principios que debe cumplir todo sistema informático.
	6. Explicar otros elementos asociados a la seguridad informática como son la autentificación y autorización.
	7. Identificar algunos obstáculos asociados a la seguridad informática en sus instituciones.
	8. Conceptos de amenazas, riesgos, vulnerabilidades e incidentes de seguridad que atentan contra la seguridad de la información.
	9. Identificar los tipos de amenazas según su origen, accidentales (causas naturales o causas laborales y/o sociales), intencionales (internas o externas).
	10. Identificar causas que pudieran provocar conductas de amenazas en sus instituciones. Algunas amenazas más comunes.
	11. Identificar vulnerabilidades asociadas a los usuarios, a la disciplina y la tecnología informática.
	12. Importancia y función de establecer políticas y medidas de seguridad administrativa, organizativa, física, lógica, legal y educativa, para prevenir posibles acciones malintencionadas o no, que se puedan causar daños a otros usuarios o al sistema informático de una institución.

	13. Analizar el marco legal vigente en Cuba en relación con las TI y sus principales aspectos abordados, que inciden en su responsabilidad personal y de las instituciones.
	14. Explicar algunos aspectos del plan de seguridad informática, como documento rector de la política de seguridad informática de una institución y sus implicaciones en los usuarios de las TI.
	15. Definir las normas éticas para el trabajo con las TI de las instituciones con los aspectos éticos que deben tenerse en cuenta cuando se accede a un sistema informático.

Tema	**Contenido**
2	1. Concepto de hacker, cracker, ejemplo de casos de sus formas de actuar.
	2. Concepto de ingeniería social, identificar ejemplos donde se pone de manifiesto.
	3. Algunas manifestaciones de hechos de ingeniería social. Análisis de casos
	4. Concepto de programa maligno
	5. Conceptos de los distintos tipos de Programas Malignos. Virus informático, Gusanos, Caballo de Troya, Hoax, Correos basura (Spam), entre otros.
	6. Tipos de virus según sus manifestaciones. Análisis de casos y principales causas de su incremento. Algunas sugerencias de cómo protegerse de los virus informáticos.
	7. Ejemplos de algún software antivirus que son utilizados en las instituciones, políticas establecidas en Cuba para el uso. Algunas sugerencias de que se debe hacer en caso de estar infestado.
	8. Los principales tipos de virus reportados en Cuba.
	9. Actualización del sistema operativo y antivirus que utilizan en las instituciones. Algunos consejos o procedimientos para realizarlo.
	10. Medidas de seguridad establecidas para el uso y la protección de la información en los dispositivos externos, uso del correo electrónico, mensajería instantánea e Internet.
	11. Amenazas que acarrean los sistemas de mensajería instantánea.
	12. Amenazas en la navegación por Internet. Algunos consejos para la navegación por sitios seguros.
	13. Medidas para garantizar el uso efectivo de claves de acceso y sus normas de uso, política de pantalla y de escritorios limpios, implementación de permisos a los archivos y carpetas, protector de pantalla o bloqueo de pantalla con claves y la configuración de sesiones de trabajo para diferentes usuarios, en correspondencia con las facilidades que provee el sistema operativo que se utiliza.

	14. Importancia de las salvas de información como recurso de recuperación ante contingencias fatales. Sugerencias de como organizar este proceso por los usuarios.
	15. Importancia de detectar y reportar incidentes informáticos. Cómo proceder.

Tema	Contenido
3	1. Configuración e implementación de permisos en archivos y carpetas
	2. Configuración de sesiones de trabajo, protector o bloqueador de pantalla con claves
	3. Herramientas administrativas o de seguridad del sistema operativo que se utiliza (Visor de sucesos para controlar los accesos).
	4. Instalación y configuración del antivirus que utilicen en la institución. Formas de actualización.
	5. Configuración de directivas, políticas o herramientas de seguridad en el sistema operativo utilizado.
	6. Configuración de normas de seguridad para las aplicaciones ofimáticas y el uso de las macro y virus de este mismo nombre. Ventajas y desventajas.
	7. Configuración del gestor de correo electrónico para recibir o enviar mensajes habilitando la opción texto sin formato, con está opción garantizamos alguna protección a los gusanos que se esconden en el código HTML del mensaje de correo electrónico.
	8. Configuración del gestor de correo electrónico para desactivar la opción de vista previa, evita infestarnos con códigos malignos que se encuentran en el cuerpo del mensaje.
	9. Algunas recomendaciones para el uso de correo electrónico, normas que se deben cumplir por usuarios.
	10. Configuración del navegador de Internet, zonas de Internet, sitios de confianza y sitios restringidos, configurando el nivel de seguridad en cada zona, se recomienda media, alto, nunca usar el nivel más bajo, además se recomienda cambiar los siguientes parámetros en la opción Internet- Nivel personalizado, la secuencias de comandos Active X, descargar los controles no firmados para Active X, inicializar y activar la secuencia de comandos de los controles de Active X no marcados como seguros y ejecutar controles y complementos de Active X, en todos los casos activar la opción preguntar.
	11. Configuración del navegador de Internet para controlar el acceso de las Cookies, que son un valioso mecanismo para identificar las áreas de interés y los hábitos de utilización de páginas Web por parte de los usuarios Ej. nombre y contraseña, productos que más le interesan eliminación de ficheros temporales.

Tema	Contenido
4	1. Conocer la metodología para la implementación del Programa de Seguridad Informática en sus instituciones.

	2. Saber identificar aquellos aspectos importantes que deben formar parte del Programa de Seguridad Informática de su institución.

Sistema de evaluación

La evaluación del curso se llevará a cabo de forma individual y grupal, tomando en consideración la información procedente de:

- Las actividades individuales y grupales programadas durante el desarrollo del curso, de forma sistemática.
- Las evaluaciones parciales al finalizar cada tema del curso.
- La evaluación final del curso.

Los resultados de todas estas actividades y evaluaciones, deberán ser enviados al profesor en las fechas indicadas en el calendario de actividades, pues de lo contrario, no serán evaluadas y por lo tanto no recibirán ninguna puntuación.

La calificación final de cada tema se realizará de forma sumativa, es decir, teniendo en consideración todas las actividades desarrolladas, y la evaluación final orientada.

La calificación final del curso se realizará de forma similar, pues se tendrán en cuenta las evaluaciones finales de cada tema y la tarea final del curso.

Sugerencias:

- Evita acumular trabajos y procura que sean realizados con claridad, sencillez, precisión y concordancia.
- Conserva todos los trabajos, pues te servirán para la actividad final del curso y además será una experiencia que podrás compartir en tu vida profesional.
- Establece contacto con tus colegas, ya sea de manera personal o electrónica, con el fin de enriquecer tus ideas, pero no olvides que el trabajo es personal.
- Instaura una comunicación con el profesor para aclarar dudas y recibir la orientación que necesites.

Bibliografía

La bibliografía general para el estudio de este curso está compuesta por los materiales que a continuación se relacionan:

Bibliografía

1. Adiestramiento "Seguridad en las Tecnologías de la Información". Empresa SEGURMATICA del Ministerio de la Informática y las Comunicaciones, MAYO 2009.
2. Adiestramiento "Los Programas Malignos y la Seguridad en el Correo Electrónico". Empresa SEGURMATICA del Ministerio de la Informática y las Comunicaciones, MAYO 2009.
3. Adiestramiento "Elaboración de Planes de Seguridad Informática". Empresa SEGURMATICA del Ministerio de la Informática y las Comunicaciones, MAYO 2009.
4. Adiestramiento " Introducción a la Seguridad en Redes". Empresa SEGURMATICA del Ministerio de la Informática y las Comunicaciones, noviembre 2010.
5. Arcert, Manual de Seguridad en Redes. Coordinación de Emergencia en Redes y Telecomunicaciones. Administración Pública Argentina, 2006.
6. Arcert, Manual del instructor en seguridad de la información. Versión 1.0. Coordinación de Emergencia en Redes y Telecomunicaciones. Administración Pública Argentina, – Noviembre 2007
7. Borghello, Cristian, F: Tesis Seguridad Informática sus implicaciones e Implementación, Argentina, 2001. Materia Digital.

8. Cano Murillo, Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la UDLA. Tesis Maestría. Ciencias con Especialidad en Ingeniería en Sistemas Computacionales. Departamento de Ingeniería en Sistemas Computacionales, Escuela de Ingeniería, Universidad de las Américas, Puebla. Mayo.2001.

9. Cerini María Dolores y Prá, Pablo Ignacio. Plan de Seguridad Informática, Universidad Católica de Córdoba, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, Octubre 2002

10. Cobo Romaní, Cristóbal, Tesis doctoral: Organización de la información y su impacto en la usabilidad. Facultad de Ciencias de la Comunicación de la Universidad Autónoma de Barcelona. Departamento de Comunicación Audiovisual y Publicidad. Ciudad de México, marzo de 2005, México.

11. Elinos Farias, M., Altamirano, C. Perfil del Oficial de Seguridad Informática. Universidad Autónoma de México. 2003. Material digital.

12. Entrenamiento en Seguridad Informática. Empresa DISAIC del Ministerio de la Industria Sidero - mecánica. Abril 2010.

13. Evento Nacional de Seguridad Informática. CD de Ponencias, Segurmatica-Cuba, noviembre 18-20-2008.

14. Lizama Mendoza J, y Farias-Elinos, M. Analfabetismo digital y sus implicaciones en la Seguridad Informática. Facultad de Ciencias Políticas, Universidad Nacional Autónoma de México, 2003

15. Montesino Perurena, Raydel. Gestión de la Seguridad Informática: de la Teoría a la Práctica. Ponencia presentada en el evento Internacional Informática 2009.

16. Espinosa María P, Pinzón Olmedo, Freddy, Identificación de vulnerabilidades, análisis forense y atención a incidentes de seguridad en los servidores de la UTPL. Universidad Católica de Loja, 2007.

17. Pérez González, Daniel. Tesis de Doctorado, Contribución de las Tecnologías de la Información a la generación de valor en las organizaciones. Un modelo de análisis desde la gestión del conocimiento, la productividad y la excelencia en la gestión. Universidad de Cantabria 2008. Material digital.

18. Ramió Aguirre, Jorge, Proyecto Criptored y el Desarrollo de la Seguridad Informática en Ibero América. Universidad de Campinas – Brasil-Octubre de 2003.

19. Ramió Aguirre, Jorge. Desarrollo de la Seguridad Informática en España, su Incidencia en la Enseñanza Universitaria y CriptoRed, diciembre de 2002. Material digital.

20. Resoluciones 6/96 del Ministerio del Interior. Reglamento sobre la Seguridad Informática

21. Resolución 204/96 del Ministerio de la Industria Sidero Mecánica sobre la seguridad y protección de la información oficial.

22. Resolución 18/2001 MINED Perfil de Técnico medio en Informática.

23. Resolución .188/2006 del Ministerio del Trabajo y Seguridad Social sobre los Reglamentos Disciplinarios Internos del 21 de agosto de 2006

24. Resolución 127/07 Ministerio de la Informática y las Comunicaciones. Reglamento de Seguridad para las Tecnologías de la Información.

25. Resolución 176/07 MINED Reglamento de Seguridad Informática en la Actividad Educacional del Ministerio de Educación.

26. Rodríguez Cuervo, A Miguel, ponencia presentada en el evento Internacional COMPUMAT, titulada " La Superación Profesional en Seguridad Informática", CD-ROM con ISSN 1728-6042, La Habana Cuba, noviembre 2009.

40. Rodríguez Cuervo, A Miguel, trabajo publicado en la Revista IPLAC titulado "La seguridad informática una necesidad en la docencia universitaria", RNPS No. 2140 / ISSN 1993-6858. enero – abril 2010.

41. Rodríguez Cuervo, A Miguel, ponencia presentada en el evento Internacional Didáctica de las Ciencias, titulada "La Educación en Seguridad Informática". Palacio de las Convenciones, Cuba, ISBN 978-959-18-0541-6, 2010

42. Rodríguez Cuervo, A Miguel, Diapositivas del Curso Elementos Básicos de Seguridad Informática, IPLAC 2010

43. Rodríguez Cuervo, A Miguel, Libro digital Elementos Básicos de Seguridad Informática, IPLAC 2010

44. Rodríguez Cuervo, A Miguel, Ponencia presentada en el evento nacional de seguridad informática del la Empresa Segurmatica del MIC. ¿Por qué y para qué la Educación en seguridad informática?., noviembre del 2010

45. de Seguridad Informática, IPLAC 2010

46. Universidad Politécnica de Madrid, Plan de estudios y temario de la asignatura seguridad informática, ingeniero técnico en informática de gestión Escuela Universitaria de Informática, 2007. Material digital

47. Universidad Pontificia de Madrid. Curso de Doctorado, Seguridad en Redes de Ordenadores, 2007, Material digital.

48. Universidad Pontificia Bolivariana. Especialización en Seguridad Informática Facultad de Ingeniería Informática, Febrero 2008, Materia Digital.

Orientaciones para el estudio

A continuación se propone un conjunto de actividades de aprendizaje, para cada uno de los temas y unidades didácticas que conforman el programa de estudio de este curso, por lo que le sugerimos que antes de comenzar a resolverlas, realicen una consulta de todos los materiales, básicos y complementarios, que se indican de forma general para el curso y de forma específica para cada uno de los temas. De igual forma se debe proceder para solucionar los ejercicios de autoevaluación orientados, los cuales no aparecen en la presente guía porque se muestran directamente en cada uno de los temas y unidades del curso en Moodle.

Tema 1: Introducción a los fundamentos de la Seguridad Informática.

Objetivo:

Que los participantes logren:

Argumentar los fundamentos de la seguridad informática a partir del reconocimiento de los objetivos y conceptos principales que la rigen.

Contenidos:

- Conceptos de información y datos.
- Clasificación de la información según su importancia.
- Concepto de sistema informático.
- Concepto de seguridad Informática y sus principales objetivos.
- Conceptos de disponibilidad, confidencialidad e integridad de la información que se procesa, intercambie, reproduzca o conserve a través de las tecnologías informáticas, como principios que debe cumplir todo sistema informático.
- Explicar otros elementos asociados a la seguridad informática como son la autentificación y autorización.
- Identificar algunos obstáculos asociados a la seguridad informática en sus instituciones.
- Conceptos de amenazas, riesgos, vulnerabilidades e incidentes de seguridad que atentan contra la seguridad de la información.
- Identificar los tipos de amenazas según su origen, accidentales (causas naturales o causas laborales y/o sociales), intencionales (internas o externas).
- Identificar causas que pudieran provocar conductas de amenazas en sus instituciones. Algunas amenazas más comunes.
- Identificar vulnerabilidades asociadas a los usuarios, a la disciplina y la tecnología informática.

- Importancia y función de establecer políticas y medidas de seguridad administrativa, organizativa, física, lógica, legal y educativa, para prevenir posibles acciones malintencionadas o no, que se puedan causar daños a otros usuarios o al sistema informático de una institución.
- Analizar el marco legal vigente en Cuba en relación con las TI y sus principales aspectos abordados, que inciden en su responsabilidad personal y de las instituciones.
- Explicar algunos aspectos del plan de seguridad informática, como documento rector de la política de seguridad informática de una institución y sus implicaciones en los usuarios de las TI.
- Definir las normas éticas para el trabajo con las TI de las instituciones con los aspectos éticos que deben tenerse en cuenta cuando se accede a un sistema informático.

Orientación para el estudio y el desarrollo de actividades:

1. Lea y estudie detalladamente en la presentación "Tema 1", que es el material básico de este tema.
2. Para profundizar en estos contenidos, le sugiero que consulte además, los materiales complementarios puestos a su disposición en este tema en la carpeta Documentación.
3. Debe revisar también otros materiales que usted pueda encontrar, ya sea de forma impresa o en formato digital.
4. Intercambie sus anotaciones e interpretaciones de lo estudiado, con el resto del grupo. De esta forma cada uno podrá exponer sus propios criterios como resultado de su autopreparación y a la vez enriquecer y actualizar sus conocimientos.
5. Sobre sus dudas y otros aspectos de consolidación del material de estudio, comentaremos a través del chat, por lo que debe estar atento a la llamada que se realizará en la fecha y hora establecida.
6. Elabore una lista de preguntas que propicien el intercambio con el profesor, con sus compañeros, y si es posible, con otros colegas. Estas preguntas le servirán para promover el debate en el foro.
7. Realice las actividades del TEMA 1.

Tema 2: La seguridad informática en las actividades cotidianas.

Objetivo:

Que los participantes logren:

Identificar las amenazas que acarrean los sistemas informáticos y conocer los procedimientos correspondientes.

Contenidos:

1. Concepto de hacker, cracker, ejemplo de casos de sus formas de actuar.
2. Concepto de ingeniería social, identificar ejemplos donde se pone de manifiesto.
3. Algunas manifestaciones de hechos de ingeniería social. Análisis de casos
4. Concepto de programa maligno
5. Conceptos de los distintos tipos de Programas Malignos. Virus informático, Gusanos, Caballo de Troya, Hoax, Correos basura (Spam), entre otros.
6. Tipos de virus según sus manifestaciones. Análisis de casos y principales causas de su incremento. Algunas sugerencias de como protegerse de los virus informáticos.
7. Ejemplos de algún software antivirus que son utilizados en las instituciones, políticas establecidas en Cuba para el uso. Algunas sugerencias de que se debe hacer en caso de estar infestado.
8. Los principales tipos de virus reportados en Cuba.

9. Actualización del sistema operativo y antivirus que utilizan en las instituciones. Algunos consejos o procedimientos para realizarlo.
10. Medidas de seguridad establecidas para el uso y la protección de la información en los dispositivos externos, uso del correo electrónico, mensajería instantánea e Internet.
11. Amenazas que acarrean los sistemas de mensajería instantánea.
12. Amenazas en la navegación por Internet. Algunos consejos para la navegación por sitios seguros.
13. Medidas para garantizar el uso efectivo de claves de acceso y sus normas de uso, política de pantalla y de escritorios limpios, implementación de permisos a los archivos y carpetas, protector de pantalla o bloqueo de pantalla con claves y la configuración de sesiones de trabajo para diferentes usuarios, en correspondencia con las facilidades que provee el sistema operativo que se utiliza.
14. Importancia de las salvas de información como recurso de recuperación ante contingencias fatales. Sugerencias de cómo organizar este proceso por los usuarios.
15. Importancia de detectar y reportar incidentes informáticos. Cómo proceder.

Orientación para el estudio y el desarrollo de actividades:

1. Lea y estudie detalladamente en la presentación "Tema 2", que es el material básico de este tema.
2. Para profundizar en estos contenidos, le sugiero que consulte además, los materiales complementarios puestos a su disposición en este tema en la carpeta Documentación.
3. Debe revisar también otros materiales que usted pueda encontrar, ya sea de forma impresa o en formato digital.
4. Intercambie sus anotaciones e interpretaciones de lo estudiado, con el resto del grupo. De esta forma cada uno podrá exponer sus propios criterios como resultado de su autopreparación y a la vez enriquecer y actualizar sus conocimientos.
5. Sobre sus dudas y otros aspectos de consolidación del material de estudio, comentaremos a través del chat, por lo que debe estar atento a la llamada que se realizará en la fecha y hora establecida.
6. Elabore una lista de preguntas que propicien el intercambio con el profesor, con sus compañeros, y si es posible, con otros colegas. Estas preguntas le servirán para promover el debate en el foro.
7. Realice las actividades del TEMA 2.

Tema 3: Algunas configuraciones en herramientas y aplicaciones informáticas.

Objetivo:

Que los participantes logren:

Demostrar las diferentes formas de configurar de manera eficiente y segura las aplicaciones y herramientas informáticas para el tratamiento de la información docente e investigativa que se procesa, intercambie, reproduzca o conserve a través de las tecnologías informáticas.

Contenidos:

- Configuración e implementación de permisos en archivos y carpetas
- Configuración de sesiones de trabajo, protector o bloqueador de pantalla con claves
- Herramientas administrativas o de seguridad del sistema operativo que se utiliza (Visor de sucesos para controlar los accesos).
- Instalación y configuración del antivirus que utilicen en la institución. Formas de actualización.
- Configuración de directivas, políticas o herramientas de seguridad en el sistema operativo utilizado.

- Configuración de normas de seguridad para las aplicaciones ofimáticas y el uso de las macro y virus de este mismo nombre. Ventajas y desventajas.
- Configuración del gestor de correo electrónico para recibir o enviar mensajes habilitando la opción texto sin formato, con esta opción garantizamos alguna protección a los gusanos que se esconden en el código HTML del mensaje de correo electrónico.
- Configuración del gestor de correo electrónico para desactivar la opción de vista previa, evita infestarnos con códigos malignos que se encuentran en el cuerpo del mensaje.
- Algunas recomendaciones para el uso de correo electrónico, normas que se deben cumplir por usuarios.
- Configuración del navegador de Internet, zonas de Internet, sitios de confianza y sitios restringidos, configurando el nivel de seguridad en cada zona, se recomienda media, alto, nunca usar el nivel más bajo, además se recomienda cambiar los siguientes parámetros en la opción Internet- Nivel personalizado, la secuencias de comandos Active X, descargar los controles no firmados para Active X, inicializar y activar la secuencia de comandos de los controles de Active X no marcados como seguros y ejecutar controles y complementos de Active X, en todos los casos activar la opción preguntar.
- Configuración del navegador de Internet para controlar el acceso de las Cookies, que son un valioso mecanismo para identificar las áreas de interés y los hábitos de utilización de páginas Web por parte de los usuarios Ej. nombre y contraseña, productos que más le interesan eliminación de ficheros temporales.

Orientación para el estudio y el desarrollo de actividades:

1. Lea y estudie detalladamente en la presentación "Tema 3", que es el material básico de este tema.
2. Para profundizar en estos contenidos, le sugiero que consulte además, los materiales complementarios puestos a su disposición en este tema en la carpeta Documentación.
3. Debe revisar también otros materiales que usted pueda encontrar, ya sea de forma impresa o en formato digital.
4. Intercambie sus anotaciones e interpretaciones de lo estudiado, con el resto del grupo. De esta forma cada uno podrá exponer sus propios criterios como resultado de su autopreparación y a la vez enriquecer y actualizar sus conocimientos.
5. Sobre sus dudas y otros aspectos de consolidación del material de estudio, comentaremos a través del chat, por lo que debe estar atento a la llamada que se realizará en la fecha y hora establecida.
6. Elabore una lista de preguntas que propicien el intercambio con el profesor, con sus compañeros, y si es posible, con otros colegas. Estas preguntas le servirán para promover el debate en el foro.
7. Realice las actividades del TEMA 3.

Tema 4: Metodología para la implementación del programa de seguridad informática en las instituciones del MINED.

Objetivo:

Que los participantes logren:

Conocer la metodología para la implementación del Programa de Seguridad Informática de manera eficiente en las instituciones del MINED.

Contenidos:

- Conocer la metodología para la implementación del Programa de Seguridad Informática en sus instituciones.

- Saber identificar aquellos aspectos importantes que deben formar parte del Programa de Seguridad Informática de su institución.

Orientación para el estudio y el desarrollo de actividades:

1. Lea y estudie detalladamente en las presentaciones “Tema 4” y “Tema 4a”, que es el material básico de este tema.
2. Para profundizar en estos contenidos, le sugiero que consulte además, los materiales complementarios puestos a su disposición en este tema en la carpeta Documentación.
3. Debe revisar también otros materiales que usted pueda encontrar, ya sea de forma impresa o en formato digital.
4. Intercambie sus anotaciones e interpretaciones de lo estudiado, con el resto del grupo. De esta forma cada uno podrá exponer sus propios criterios como resultado de su autopreparación y a la vez enriquecer y actualizar sus conocimientos.
5. Sobre sus dudas y otros aspectos de consolidación del material de estudio, comentaremos a través del chat, por lo que debe estar atento a la llamada que se realizará en la fecha y hora establecida.
6. Elabore una lista de preguntas que propicien el intercambio con el profesor, con sus compañeros, y si es posible, con otros colegas. Estas preguntas le servirán para promover el debate en el foro.
7. Realice las actividades del TEMA 4.